EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. When a security analysis demonstrates the existence of vulnerabilities in election equipment, there are a wealth of reasons to make those findings broadly available to the public, subject to appropriate limitations.

3. Public disclosure ensures that all jurisdictions that rely on the vulnerable equipment will be aware of the problems and able to begin mitigating them. It informs law enforcement and national security groups about forms of attack that they

should be on the lookout for. It helps jurisdictions that are procuring new equipment make better informed purchases. It ensures that vendors of other equipment that may suffer from similar problems are on notice. It provides a foundation for research and development of stronger election security mechanisms. It informs test laboratories and regulators such as the U.S. Election Assistance Commission about gaps in established testing methodologies. It also helps inform policymakers, such as state legislatures and the U.S. Congress, which is now considering several measures to overhaul election cybersecurity. Ultimately, transparency about actual election system vulnerabilities can improve public trust in elections by demonstrating that election security has been rigorously scrutinized and by helping to separate facts about real vulnerabilities (which technology and policy changes can address) from the baseless speculation and fantasy of conspiracy theorists.

4. However, it is important to make findings about vulnerabilities public in the right way, considering both the timing of the public disclosure and its content. In general, public vulnerability disclosures must "strike a careful balance between the public's interest in transparency into whether their voting systems are secure and the public's interest in being protected against the risks due to the disclosure of those

flaws."[1] Previous election security analyses have attempted to strike this balance by withholding specific details that would greatly benefit potential attackers while shedding little light for the public about the scope or nature of the security problems.

5. A prime example of how this balance has been struck is the California Secretary of State's Top-to-Bottom Review of Electronic Voting Systems (TTBR), the first comprehensive state-sponsored election security review, in which I took part as an expert. The TTBR resulted in hundreds of pages of public reports describing numerous vulnerabilities in voting systems from four major vendors.[2] Nevertheless, the authors withheld certain key details about some of the problems. In the words of the principal investigator, "Our objective was to avoid reducing the amount of access an attacker would require to attack elections. We attempted to accomplish this by omitting details that would have the effect of converting an attack that would require reverse engineering or access to the source code into one that would not. These details were relegated to a confidential appendix."[3] Project EVEREST, a similar comprehensive election security review commissioned by the Secretary of State of

---

[1] David A. Wagner, "Principal Investigator's Statement on Protection of Security-Sensitive Information," *California Top-to-Bottom Review of Voting Systems* (2007). Available at https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/state-of-protect(dw).pdf.
[2] California Secretary of State, *Top-to-Bottom Review* (2007). https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review.
[3] Ibid. 1.

Ohio, applied a similar strategy, again making hundreds of pages of detailed findings public while withholding key details in select instances.[4]

6. The computer science research community similarly recognizes that researchers who discover vulnerabilities have a professional and ethical duty to safeguard the public interest. Key to this protection is the notion of giving responsible parties an early warning about the problems before such knowledge becomes public (a so-called "disclosure window"), so that they can take remediative action. During the scientific peer review process, referees consider whether the duty to protect the public has been fulfilled and may deny or delay publication if it has not. For example, the IEEE Symposium on Security and Privacy, one of the premier scientific venues for security research, requires that:

> "Where research identifies a vulnerability (e.g., software vulnerabilities in a given program, design weaknesses in a hardware system, or any other kind of vulnerability in deployed systems), we expect that researchers act in a way that avoids gratuitous harm to affected users and, where possible, affirmatively protects those users. In nearly every

[4] Patrick McDaniel et al., "EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing" (2007). Available at https://www.eac.gov/sites/default/files/document_library/files/EVEREST.pdf.

> case, disclosing the vulnerability to vendors of affected systems, and other stakeholders, will help protect users. It is the committee's sense that a disclosure window of 45 days to 90 days ahead of publication is consistent with authors' ethical obligations."[5]

7. In preparing my expert report in this case, I did not anticipate that it might become public immediately, given the Court's existing protective order. As such, the report contains some specific details that might be dangerous in the wrong hands. I would be happy to prepare an abridged version that removes this information if the Court sees fit to make the findings public.

8. I have been attempting since January, through Plaintiffs' counsel, to meet with Dominion to confidentially discuss the vulnerabilities in my report. However, Dominion has yet to agree to meet. It would be dangerous to provide Dominion with the complete report if it were then disclosed through discovery in the company's various ongoing defamation suits to anyone who might misuse it.

---

[5] IEEE Symposium on Security and Privacy, "Call for Papers" (2021). Available at https://www.ieee-security.org/TC/SP2022/cfpapers.html.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 12th day of July, 2021 in Rushland, Pennsylvania.

J. ALEX HALDERMAN